COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-2766
PHONE: (213) 974-8301 FAX: (213) 626-5427

J. TYLER McCAULEY
AUDITOR-CONTROLLER

May 27, 2005

To: Supervisor Gloria Molina, Chair
Supervisor Yvonne B. Burke
Supervisor Zev Yaroslavsky
Supervisor Don Knabe
Supervisor Michael D. Antonovich

From: J. Tyler McCauley
Auditor-Controller

Subject: **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY COMPLIANCE STATUS REPORT- NOVEMBER 13, 2004 THROUGH APRIL 30, 2005**

This report is collateral to the April 11, 2005 status report submitted to your Board by the Chief Information Office (CIO) regarding compliance activities with Health Insurance Portability and Accountability Act (HIPAA) Transactions and Code Sets Rules. This report focuses on the County's progress in implementing and complying with HIPAA's Privacy Rule, which is the responsibility of the Chief Privacy Officer in the Auditor-Controller.

Although the County is moving closer toward full compliance, there are challenges related to the complexity of implementing the mandates of the program that require ongoing assessment coupled with the enormous task of providing employee training. Nonetheless, our goal remains to further enhance the program by increasing awareness and improving its efficiency and effectiveness.

HIPAA Privacy Compliance Reviews

During this reporting period, my Chief Privacy Officer (AC-CPO) conducted reviews of DHS' Public Health's Central and Hollywood-Wilshire Health Centers (Health Centers) located within Service Planning Area 4; and, a compliance review of the Probation Department's Dorothy Kirby Center was performed. The results are detailed in the HIPAA Privacy Review Summary Report, (Attachment 1).

Overall, our findings show these facilities are significantly non-compliant. Further, because various discrepancies are assessed as "Major," this presents a risk to the departments since employees may inadvertently disclose protected patient information. Health Centers and Dorothy Kirby have acknowledged these deficiencies and mitigated most, if not all, at the date of this report.

The number of privacy complaints submitted to either the AC-CPO or directly to the departments remain low. However, some of the complaints identified valid and discerning privacy violations that point to the need for further administrative training in the area of policies and procedures. County Counsel and related departments' management are involved with resolving these complaint issues.

HIPAA Privacy Complaints and Business Associate Agreement Concerns

On February 9, 2005, the Office of Civil Rights (OCR), the federal agency responsible for enforcing HIPAA Privacy, sent a letter to the Chief Privacy Officer regarding a complaint from outside of the County. The complaint alleged that the Department of Health Services (DHS) and the Martin Luther King/Drew Medical Center committed privacy violations. After a thorough investigation, the AC-CPO submitted a response letter on February 22, 2005 to OCR refuting the allegations. OCR has since requested additional facts and a response was provided. We are waiting for notice that the explanation and mitigation issues are satisfactory in order to close this case.

Although our findings show that DHS did not commit a HIPAA Privacy violation pursuant to OCR's letter of complaint, it was determined that DHS breached the provisions of the HIPAA Business Associate Agreements' (BAAs) guidelines and their own departmental policies. On April 18, 2005, the AC-CPO sent a letter to DHS' Privacy Officer which identified the improper disclosure of Protected Health Information (PHI) to physicians outside of DHS' designated workforce. The letter stated that because DHS' Office of Managed Care is a health care provider and is a covered health plan under HIPAA, it must have separate BAAs than those from DHS. Corrective action for these violations was requested no later than May 30, 2005.

Other Auditor-Controller Countywide Security Audit and Compliance Duties

In a previous HIPAA Privacy Compliance memo to your Board, it was noted that on July 29, 2004, your Board approved and adopted nine Information Technology (IT) and Security Policies that were presented by the CIO. On August 9, 2004, the CIO distributed a letter to each department head informing them that these policies were effective immediately and were applicable to all departments. Specifically, Policy 6.108 *Security Auditing and Compliance* creates a new responsibility and duty for the Auditor-Controller which is to conduct security audits on all departmental information technology

systems throughout the County. We estimate that there are over 150,000 computing devices and over 25,000 associated unique software application versions that would require such security audits.

This new policy presents a concern since this is an immense administrative and financial burden that was not previously planned or fiscally forecasted in the 2005-06 Fiscal Year proposed budget process. While the Auditor-Controller agrees with the intent of the policy and also believes that this underlining task falls to the Auditor-Controller, the immediate challenge is the lack of staff and resources to carry out these new duties. On April 22, 2005, the AC-CPO distributed a letter to the Information Technology (IT) Board deputies that presented options and recommendations for managing this new initiative. We will report our approach for implementation to your Board in future Board status reports.

New Appointment of Privacy Officer

My Chief Privacy Officer, Mr. Glen Day, left County service to pursue other opportunities with private industry. Because this position is federally mandated, I have therefore hired a replacement, Ms. Linda T. McBride, J.D., to assume the responsibilities of the position. Prior to Linda joining the Auditor-Controller, she spent ten years with the Chief Administrative Office. I believe that Linda's prior County experience coupled with her legal education will be an asset to this Department and our efforts to ensure the County complies with HIPAA regulations. Her transition to this Department was effective May 16, 2005.

Summary

The County's HIPAA Privacy Program continues to increase a global perspective of health privacy issues as it relates to both health care providers and health plans. Primarily due to the impact of the Privacy Rule, members of the health care community are more aware of protecting their patients' health information. All HIPAA impacted departments are encouraged to keep a strong vigilance regarding and Security mandates to ensure the County continues to improve and enhance its compliance efforts.

The next semi-annual report is expected to be submitted in October, 2005. However, if circumstances warrant earlier reporting, we will submit a report(s) on an as-needed basis. If you have questions or require additional information, please contact me at (213) 974-0383, or your staff may contact Linda McBride at (213) 974-2166.

JTM:WW:LTM

Attachment

c: David E. Janssen, Chief Administrative Officer
Leroy D. Baca, Sheriff
Raymond Fortner, County Counsel
Stephanie Farrell, County Counsel
Jon Fullinwider, Chief Information Officer
Alan Brusewitz, Chief Information Security Officer, Chief Information Office
Dr. Thomas Garthwaite, Director, Department of Health Services
Michael J. Henry, Director, Department of Human Resources
Paul Higa, Chief Probation Officer
Dave Lambertson, Director, Internal Services Department
Mark J. Saladino, Treasurer and Tax Collector
Dr. Marvin Southard, Director, Department of Mental Health

HIPAA Privacy Review Discrepancy Summary Report -as of May 27, 2005

Facility	Severity	Discrepancy	Status
DHS Headquarters	**Minor**	The current Minimum Necessary Policy was deemed to be ineffective since it creates a redundant administrative burden on the hospital to re-create and redefine role-based access schemes that ensures that its workforce has the proper level of access to protected health information (PHI). Harbor was able to demonstrate that they have existing policies and procedures that meet this requirement.	**DHS was previously expected to revise its policy by November 1, 2004. However, it opted to simply provide references to the applicable existing policies that detail how the Minimum Necessary program is managed. DHS is expected to provide a per hospital/agency status in May, 2005.**
	Major	DHS has no trustworthy enterprise system to adequately track HIPAA Privacy training status. The statistics in the Health Care Compliance System (HCCS), which tracks HIPAA training throughout the County, does not coincide with the statistics provided by the hospitals. The current process for tracking HIPAA training is under review within the Department of Health Services (DHS) . Recommend that DHS revise the process for maintaining the HCCS database to improve the quality of the actual training statistics.	**DHS planed to migrate its HIPAA training statistics to a new Learning Management System (LMS) starting October 2004. However, the LMS was not deployed throughout DHS. DHS needs to reconcile its personnel training status between CWTAPPS and HCCS. The Severity of this discrepancy has been upgraded to Major due to the prolonged exposure.**
DHS' Business Associate Agreements	**Major**	DHS disclosed Patient Health Information (PHI) to two physicians outside of its workforce to provide health operations services on behalf of DHS. OMC must have separate policy and procedures that are unique to a health plan and must also been viewed as a separate organization from DHS' health care operations.	**Corrective action for these violations was requested no later than May 30, 2005.**
DHS' LAC+USC Healthcare Network (Cluster Departments 160 and 161)	**Issue**	27 desktop computers within the same network segment were assessed using automated scanning tools. The scanned computers were assessed as being inadequately secured to prevent reasonable attempts to access PHI without authorization. A detailed vulnerability assessment report was submitted to the Network's Security Officer for a more explicit review. The following were identified as HIGH RISK concerns:	
	Major	8 computers had hard drives formatted with the File Allocation Table (FAT) file systems vs. the NT File Systems (NTFS). Hard drives formatted with FAT are less secure and present a higher risk for unauthorized access. NTFS also supports systems audit features that better support computer security forensic investigations.	LAC+USC converted its Windows-based file system from FAT to NTFS and made it the technical standard for new systems.
	Major	All scanned computers had multiple unauthorized access vulnerabilities due to a lack of patch management support. Many of the available patches and service packs were not installed. Some patches have been available for more than year.	LAC+USC installed the Patch Link application to manage its software patch efforts.

**** Note- Status items in BOLD are still outstanding.***

HIPAA Privacy Review Discrepancy Summary Report -as of May 27, 2005

Facility	Severity	Discrepancy	Status
DMH's Edmund D Edelman Westside Mental Health Center	**Major**	The excessive storage of paper-based health records and charts continues to be a concern. The facilities are increasing their risk of unauthorized disclosure of PHI and have an increased administrative burden for managing outdated records since there is no formal policy in which to destroy outdated health records. As presented during the February 5, 2004 Preliminary HIPAA Privacy Review, the archived storage of PHI needs to be addressed such that the facilities have a clear policy and procedure in which they can appropriately destroy paper-based PHI that no longer requires maintenance.	**In February 2004, it was recommended that DMH expeditiously draft and approve a policy and procedure for destroying outdated paper-based health records and charts. To date, the policy has not been drafted.**
	Minor	There were 26 identified computer monitors that presented PHI and were visible to patients. The Program Head mentioned that approximately 65 privacy screens were requested, but none were approved.	**On September 27, 2004, the Program Head reported that a new request for 26 privacy screens has been submitted and is awaiting approval. To date, there has been no status update.**
DMH's Arcadia Mental Health Center	**Issue**	28 local computers within the same network segment were assessed using automated scanning tools. The scanned computers were assessed as inadequately secured to prevent reasonable attempts to access PHI without authorization. A detailed vulnerability assessment report will be submitted to the DMH's Security Officer for their detailed review. The following discrepancies were identified as the HIGH RISK concerns:	
	Major	All scanned computers had multiple vulnerabilities that could permit unauthorized access due to a lack of patch management support. Many of the available patches and service packs were not installed. Some patches have been available for more than year.	On September 27, 2004, DMH reported that it purchased a new desktop management suite. Part of the suite includes an enterprise patch management component, which DMH states was deployed and operational in April, 2005.
Probation's Dorothy Kirby Center & DMH	**Major**	The Dorothy Kirby Center was inappropriately utilizing HIPAA privacy policies from DMH. Upon initial review, only a handful of policies were requested for revision to be core Dorothy Kirby policies. However, further review required the Center to create and maintain all of its own HIPAA privacy policies and procedures.	On April 22, 2005, Dorothy Kirby confirmed that all of their HIPAA privacy policies are now under their own letterhead.
	Major	Dorothy Kirby's HIPAA Privacy training program is not accurate and current. Their entire workforce has not completed training as required by HIPAA.	On April 22, 2005, Dorothy Kirby facility confirmed that it trained the remaining 12 volunteers (Clergy) who were outstanding since the review and trained additional new staff members.
	Major	Dorothy Kirby was not issuing Business Associate Agreements (BAAs) per the HIPAA Privacy Rule.	On April 22, 2005, Dorothy Kirby confirmed that it issued 4 BAAs to its appropriate vendors.
	Issue	22 local DMH computers within the same network segment were assessed using automated scanning tools. The scanned computers were assessed as being inadequately secured to prevent reasonable attempts to access PHI without authorization. A detailed vulnerability assessment report will be submitted to the DMH's Security Officer for their detailed review. The following discrepancies were identified as the HIGH RISK concerns:	
	Major	Two computers were identified as being infected with attempts to perform a denial of services.	On March 23, 2005, DMH reported that it performed a complete scan of all machines at Dorothy Kirby Mental Health Center. All outdated anti-virus signatures were updated. The two infected computers have been patched and vulnerabilities have been mitigated.
	Major	All scanned computers had multiple vulnerabilities that could permit unauthorized access due to a lack of patch management support. Many of the available patches and service packs were not installed. Some patched have been available for more than a year.	On March 23, 2005, DMH reported that it purchased Altiris desktop management suite. Part of the Altiris suite includes an enterprise patch management component. The Alteris patch management suite has been deployed at the Kirby center in an effort to prevent future vulnerabilities at the site.

**** Note- Status items in BOLD are still outstanding.***

HIPAA Privacy Review Discrepancy Summary Report -as of May 27, 2005

Facility	Severity	Discrepancy	Status
DHS' Public Health Centers (Central and Hollywood-Wilshire Health Centers within Service Planning Area 4)	Minor	The Notice of Privacy Practices (NPP) were not posted at both health centers.	On April 13, 2005, Public Health reported that it posted the NPP in key patient areas.
	Minor	Central Health Center had 3 of 62 workforce members as not competing the privacy training, based on the data in HCCS. Hollywood-Wilshire Health Center had 3 of 54 workforce members as not competing the privacy training, based on the data in HCCS.	**On April 13, 2005, Public Health reported that it is in progress of correcting.**
	Major	Various workforce members from both health centers that are nurses, physicians or medical records administrators are credited for only completing HIPAA Awareness training curriculum.	**On April 13, 2005, Public Health reported that it is in progress of correcting which includes reassigning the appropriate level of training.**
	Minor	The intake area at the Immunization Center (Hollywood) had PHI documents accessible to patients at the registration counter.	On April 13, 2005, Public Health reported that it corrected the discrepancy.
	Minor	Various computers at the health centers that process PHI were visible to patients. If not further protected, there is high likelihood that PHI may be inadvertently disclosed to patients.	On April 13, 2005, Public Health reported that it repositioned the computers and has also requisitioned privacy screens.
	Minor	All of the computers sampled had outdated anti-virus software updates in which some were outdated over two years. Outdated anti-virus software cannot protect the PHI stored on the computers against malicious data disclosure, modification or destruction.	**On April 13, 2005, Public Health reported that it is in progress of correcting in which all health centers will be in compliance by June 30, 2005.**
	Minor	All of the computers sampled had no password-enabled screensavers that would activate after a set amount of time of inactivity. At least one publicly accessible station was unattended and had PHI displayed upon the monitor.	On April 13, 2005, Public Health reported that it implemented password-enabled screensavers.
	Major	The Hollywood-Wilshire Health Center's medical records room is shared with another, non-County healthcare provider. The medical records room has a separate locked access for the Public Health records. However, there is an accessible air gap above the Public Health records door that could permit the non-County staff unauthorized access to Public Health's medical records.	On April 13, 2005, Public Health reported that it has installed a barrier over the air gap.
	Major	The Central Health Center had no fire suppression system installed in the STD Medical Records' room. No reasonable fire prevention system is installed and, in the event of a fire, the records would could be destroyed.	**On April 13, 2005, Public Health reported that it will solicit services to install a stand-alone fire suppression system in the STD Medical Records Room.**
	Major	The health centers have not performed the administrative tasks of identifying and recording the minimally required levels of access and disclosure for their workforce in accordance with their policy and procedures. The facilities are at a high risk of providing improper access or disclosure of PHI.	On April 13, 2005, Public Health reported that it corrected the discrepancy.
	Issue	53 desktop computers from the Hollywood-Wilshire Health Center were remotely assessed from the Public Health Information Services Center (Ferguson) using automated scanning tools. The scanned computers were assessed as being inadequately secured to prevent reasonable attempts to access PHI without authorization. Due to time and certain limitations, Central Health Center was not scanned for compliance.	
	Major	3 computers had accounts with blank passwords enabled. This would permit unauthorized easy access to PHI.	On April 13, 2005, Public Health reported that it corrected the discrepancy.
	Major	All scanned computers had multiple unauthorized access vulnerabilities due to a lack of patch management support. Many of the available patches and service packs were not installed.	**On April 13, 2005, Public Health reported that it is in progress of correcting. It has requisitioned software solutions to help mitigate the issues.**

**** Note- Status items in BOLD are still outstanding.***

	Major	Key events, such as user logon and directory service access, are not being audited and logged. Without auditing enabled, administrators cannot track unauthorized access attempts and breaches.	On April 13, 2005, Public Health reported that it corrected the discrepancy.

**** Note- Status items in BOLD are still outstanding.***